Concernant le point V.

1. La présente invention présente une méthode d'authentification (**revendication indépendante 1**) et un module de sécurité (**revendication indépendante 17**) permettant l'authentification de ou des applications dans un équipement mobile tant lors de leur téléchargement que de leur exécution.

2. Concernant la **revendication 1**:

2.1 Le document FR2831362, 25 Avril 2003 (2003-04-25); est considéré comme l'état de la technique le plus proche et décrit une méthode d'authentification d'au moins une application-fonctionnant dans un équipement connecté par un réseau à un serveur de contrôle, ledit équipement étant localement connecté à un module de sécurité, ladite application est chargée et/ou exécutée au moyen d'un environnement d'exécution d'applications de l'équipement et utilise des ressources stockées dans le module de sécurité, comprenant les étapes préliminaires suivantes:
- réception de données comprenant au moins l'identifiant de l'équipement et l'identifiant du module de sécurité, via le réseau, par le serveur de contrôle ,
- analyse et vérification par le serveur de contrôle des dites données,
- génération d'un cryptogramme comprenant une empreinte de l'application, des données identifiant l'équipement et le module de sécurité et des instructions destinées audit module
- transmission du dit cryptogramme, via le réseau et l'équipement, au module de sécurité,
- vérification de l'application en comparant l'empreinte extraite du cryptogramme reçu avec une empreinte déterminée par le module de sécurité

2.2 Le problème posé peut-être considéré comme étant de limiter les risques liés au fait qu'un module d'abonné soit utilisé à mauvais escient soit par des applications ne remplissant pas certains critères de sécurité, soit par des équipements mobiles ne remplissant pas certains critères de sécurité préétablis.

2.3 La solution de ce problème est proposée par la différence entre l'objet de la revendication indépendante 1 et la méthode d'authentification décrite ci-dessus,

nommément lors de l'initialisation et/ou de l'activation de l'application, le module de sécurité exécute les instructions extraites du cryptogramme et libère, respectivement bloque l'accès à certaines ressources du dit module de sécurité en fonction du résultat de la vérification propre à cette application effectuée préalablement.

Le document FR2831362 ne décrit pas ni ne suggère le problème technique et sa solution. En effet, selon ce procédé, un lien de confiance est d'abord établi entre le serveur et la carte SIM par l'échange sécurité de clés publiques, puis un achat d'une application est effectué par la transmission d'un fichier de demande par l'équipement mobile au serveur. Celui-ci encrypte partiellement ou entièrement l'application et transmet à l'équipement mobile un cryptogramme formé par la clé d'encryption et une commande, le tout crypté avec une clé publique connue de la carte SIM. L'exécution entraîne le téléchargement dans l'équipement mobile de l 'application partiellement ou entièrement encryptée par le serveur. Une fois chargée, l'application est décryptée par la clé stockée dans la carte SIM puis installée dans l'équipement mobile. Le document GB2387505 décrit un procédé similaire au document FR2831362. En conséquence, l'objet de la **revendication indépendante 1** est nouveau et inventif.

3. La **revendication indépendante 17** correspond en termes d'un module de sécurité à la méthode de la revendication 1. Par conséquent, l'objet de la revendication indépendante 17 est également nouveau et inventif.

4. Les **revendications 2 à 16** et **18** dépendent respectivement de la revendication 1 et de la revendication 17 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.